

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Inadequate Security Controls Increase Risks to DHS Wireless Networks



Office of Information Technology

OIG-04-27 June 2004



**Homeland
Security**

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, investigative, and special reports prepared by the OIG as part of its DHS oversight responsibility to identify and prevent fraud, waste, abuse, and mismanagement.

This report assesses the strengths and weaknesses of the program or operation under review. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to the OIG, and have been discussed in draft with those responsible for implementation. It is my hope that this report will result in more effective, efficient, and economical operations. I express my appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in black ink, appearing to read "Clark Kent Ervin".

Clark Kent Ervin
Inspector General

Contents

| | |
|--|----|
| Introduction..... | 3 |
| Results in Brief | 3 |
| Background..... | 4 |
| Findings... .. | 6 |
| Strengthened Security Guidance Is Needed For Wireless Network Implementation | 6 |
| Wireless Networks and Messaging Systems Are Vulnerable | 9 |
| Wireless Networks Have Not Been Certified and Accredited | 19 |
| Recommendations..... | 21 |
| Management Comments and OIG Evaluation | 22 |

Appendices

| | | |
|-------------|---|----|
| Appendix A: | Purpose, Scope, and Methodology..... | 25 |
| Appendix B: | Management’s Response..... | 27 |
| Appendix C: | Wireless Technology Standards and Functionality | 33 |
| Appendix D: | DHS Wireless Capabilities..... | 34 |
| Appendix E: | Report Distribution | 35 |
| Appendix F: | Major Contributors to the Report..... | 36 |

Abbreviations

| | |
|---------|--|
| 802.11x | Wireless Fidelity: 802.11a, 802.11b, and 802.11g |
| CBP | Bureau of Customs and Border Protection |
| CIS | Bureau of Citizenship and Immigration Services |
| ICE | Bureau of Immigration and Customs Enforcement |
| CIO | Chief Information Officer |
| C&A | Certification and Accreditation |

Contents

| | |
|----------|--|
| DHS | Department of Homeland Security |
| DMZ | Demilitarized Zone |
| EP&R | Emergency Preparedness and Response |
| FISMA | Federal Information Security Management Act |
| Handbook | The DHS IT Security Program Handbook for Sensitive Systems |
| IDS | Intrusion Detection System |
| IrDA | Infrared |
| ISSO | Information System Security Officers |
| IT | Information Technology |
| MAC | Media Access Control |
| MD | Management Directive |
| NIST | National Institute of Standards and Technology |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| PDA | Personal Digital Assistant |
| SP | Special Publication |
| SSID | Service Set Identifier |
| TSA | Transportation Security Administration |
| USCG | United States Coast Guard |
| USSS | United States Secret Service |
| WEP | Wired Equivalent Privacy |

Department of Homeland Security *Office of Inspector General*

Introduction

The Office of Inspector General (OIG) evaluated whether Department of Homeland Security (DHS) and its components¹ have implemented adequate security controls to protect data transmitted on wireless networks and devices. This audit included an evaluation of the security policies and procedures for the administration, configuration, and use of sensitive but unclassified DHS wireless networks.

The objective was to determine whether DHS developed adequate security policies, established oversight procedures, and implemented sufficient security measures to ensure that wireless networks and devices are secure. Work was conducted at DHS' Office of the Chief Information Officer (CIO) and selected components. Fieldwork was performed at DHS facilities from October 2003 through January 2004. See Appendix A for a discussion of our purpose, scope, and methodology.

Results in Brief

DHS has not provided sufficient guidance to its components or established adequate controls necessary to implement its wireless program. Specifically: (1) wireless policy is incomplete, (2) procedures do not establish a sound baseline for wireless security implementation, and (3) the National Wireless Management Office is not exercising its full responsibilities in addressing DHS' wireless technologies. Further, DHS has not established adequate security measures to protect its wireless networks and devices against security risks. Finally, although the DHS security policy requires certification and accreditation (C&A) for its systems to operate, none of the wireless systems reviewed had been certified or accredited. As a result of these wireless network exposures, DHS cannot ensure that the sensitive information processed by its wireless systems are effectively protected from unauthorized accesses and potential misuse.

¹ DHS components are defined as Directorates (including organizational elements and bureaus) and critical agencies.

Our report includes five recommendations that will assist DHS in remedying the deficiencies that we identified. Specifically, the DHS CIO should:

- Define the conditions and limitations for using wireless technologies in the DHS security policy.
- Update the DHS Information Technology (IT) Security Program Handbook for Sensitive Systems (Handbook) to include implementation procedures required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-48 for the use of wireless technologies.
- Require the National Wireless Management Office (WMO) to provide the necessary oversight and guidance to align components' wireless programs with DHS' wireless goals.
- Implement a standardized configuration for wireless technologies on DHS networks.
- Complete a C&A for each DHS system.

In response to our draft report, the DHS CIO agreed and has already taken steps to implement each of the above recommendations. However, the DHS CIO disagreed that the National Wireless Management Office is not exercising its full responsibilities. Based on our assessment of the CIO's response, we continue to maintain our conclusion that oversight by the WMO of wireless functionality within DHS needs to be improved. DHS' response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

Wireless technologies can enhance the productivity of DHS employees. Enhanced functionality and increases in the number and types of available applications have dramatically increased the use and usefulness of wireless devices. Wireless devices have addressed user requirements for immediate communication, service, and greater productivity. In the past five years, there has been a dramatic evolution in wireless technologies, standards, and implementation practice. These changes may expose sensitive information systems to security vulnerabilities.

The use of wireless technology has introduced new security risks to a wired network, such as unauthorized access to data through eavesdropping² or theft. Highly portable, handheld wireless devices, such as personal digital assistants³ (PDA) and wireless messaging devices, can contain sensitive information that is easily retrievable, especially if the device is lost or stolen. Eavesdropping can result in a hacker gaining unauthorized access to DHS' wired network. Further, the flexibility and portability of wireless technology and devices increases the need for security. One concern is data interception. Hackers can intercept radio signals by eavesdropping on the transmission, possibly compromising sensitive data stored on laptop computers, PDAs, and other wireless handheld devices. The introduction of these vulnerabilities increases the need to develop adequate policies and procedures and to implement strong security controls to mitigate risks associated with wireless devices and networks.

The most common communication standards used by wireless devices are:

- 1) 802.11x⁴
- 2) Bluetooth
- 3) Infrared (IrDA)

The 802.11x devices form a wireless local area network by connecting through an access point or to other 802.11x devices. Today, most laptop computers are equipped with 802.11x chipsets and IrDA ports, which give these devices wireless functionality. Recently, projectors have included the capability to use the 802.11x wireless technology communication standard. "Bluetooth" is primarily used on handheld devices such as PDAs. Some new generation printers come with IrDA ports, 802.11x, and Bluetooth chipsets already built-in. See Appendix C for more information on wireless technology standards and functionality.

The tragic events of September 11, 2001, underscored the need for critical personnel and senior management to have the capability to communicate sensitive information and management decisions securely during emergencies. On this date, excessive call volume overburdened the cellular telephone system, but

² "Eavesdropping" is the operation of capturing data by an unintended party; in addition to invasion of privacy, it may also lead to other attacks such as impersonation, session hijacking, packet spoofing, and internet sharing by unauthorized parties.

³ A handheld computer that stores and organizes personal information. Data is synchronized between a user's PDA and desktop computer by cable or wireless transmission.

⁴ The Institute of Electrical and Electronics Engineers 802.11 standards, such as 802.11a, 802.11b, and 802.11g; and implies Wireless Fidelity or Wireless Local Area Network.

the Blackberry® communication services were able to function. DHS uses Blackberry® devices as its primary wireless messaging service.

The *Federal Information Security Management Act (FISMA) of 2002*, Title III, E-Government Act of 2002, P.L. 107-347, December 17, 2002, requires each agency to develop, document, and implement an agency-wide information security program, to provide security for the information and information systems, including wireless systems, that support the operations and assets of the agency. Policies should ensure that information security is addressed throughout the life cycle of each agency information system and determine minimally acceptable system configuration requirements.

Findings

Strengthened Security Guidance Is Needed For Wireless Network Implementation

DHS has not provided sufficient guidance on wireless implementation to its components. Specifically: (1) wireless policy is incomplete and remains in draft; (2) implementation procedures do not establish a sound baseline for wireless security; and, (3) the National Wireless Management Office is not exercising its full responsibilities in overseeing DHS' wireless technologies. As a result, the lack of adequate guidance has diminished the effectiveness of controls implemented to protect DHS networks.

DHS Wireless Policy Is Incomplete

Although DHS established an *Information Technology Security Program* policy, Management Directive (MD) 4300A, to include wireless communication technologies and devices, it does not cover Bluetooth technology and remains in draft.⁵ Without specific policy, IT security managers are less likely to address the risks associated with the use of Bluetooth technology which is designed to connect disparate devices to form an ad hoc network. Further, components have not established their own IT security policies including wireless technology.

When drafting its wireless communications policy, DHS officials omitted Bluetooth technology, because they concluded that it did not pose a significant

⁵ At the time of our review, MD 4300A was in draft; however, as of February 9, 2004, this MD was formally issued.

risk. However, other federal and wireless industry authorities have issued security notices on Bluetooth vulnerabilities. As Bluetooth functionality is added to more devices and continues to gain widespread use, DHS must address the security vulnerabilities associated with the use of Bluetooth technology. Many devices such as laptop computers, cellular phones, printers, PDAs, cameras, and other peripheral devices have Bluetooth technology built-in.

DHS and its components share the responsibility for developing, implementing, and managing their wireless communications. While the DHS Office of the CIO is responsible for the oversight and management of its wireless program, the components, using the DHS IT security policy as a baseline, were required to develop their own IT security policies, standards, and guidelines to include wireless activities. MD 4300A required each component to provide draft directives and procedures to the DHS Chief Information Security Officer by November 30, 2003. Only three of the eight components covered in our review - Emergency Preparedness and Response (EP&R), Transportation Security Administration (TSA), and United States Coast Guard (USCG) - prepared draft security policies for wireless technology. Although these policies have been drafted, they do not include all of the requirements contained in the DHS security policy or the NIST SP 800-48. The remaining five components lacked policies to address wireless communications.

Implementation Procedures Can Be Improved

The DHS Handbook⁶ does not include many of the required controls for 802.11x and wireless messaging systems as prescribed by NIST SP 800-48. Further, the handbook does not define the necessary security controls for the implementation and use of Bluetooth technology. Consequently, components may lack sufficient guidance to implement effective security controls for wireless networks and devices.

The purpose of the DHS Handbook is to provide procedures for implementing the requirements of the DHS IT Security Program. To support the security of wireless technology, the handbook refers to various NIST publications. The NIST SP 800-48, *Wireless Network Security*, provides security guidelines and procedures for 802.11x, Bluetooth, and handheld devices. The handbook did not include any reference on the use of Bluetooth technology. As a result, critical security management practices and controls for maintaining and operating a secure

⁶ Version 1.4, dated December 16, 2003.

wireless network, recommended by NIST SP 800-48, were not incorporated into the handbook, including:

- Definitions of the approved uses of wireless networks.
- Standards for hardware and software configurations for portable electronic devices.
- Conditions and limitations for handheld devices, such as authorized locations or the use of public “hot spots.”
- Requirements for reporting and deactivating lost or stolen laptops and handheld devices and disposing of wireless devices.
- Criteria for the use of handheld device features such as wireless radio frequency transmission, peer-to-peer⁷ communication, and Internet connectivity.
- Requirements to monitor the wireless industry for the release of new products with improved security or changes in wireless standards affecting security.
- Requirements to review security alerts and advisories relevant to wireless technology to identify vulnerabilities applicable to the DHS environment.

The National Wireless Management Office Is Not Exercising Its Full Responsibilities

The National Wireless Management Office currently does not oversee all DHS wireless functionality. The office was created on March 25, 2003, by MD 4100.1, to oversee all wireless technology and establish wireless goals to improve homeland security, reduce technology costs, and ensure interoperability of systems. Although the National Wireless Management Office was to coordinate and develop policy and strategy for all DHS wireless technologies, at present, its primary focus is on land mobile radio systems. The National Wireless Management Office does not provide current oversight of wireless implementation within DHS. The National Wireless Management Office is

⁷ Peer-to-peer messages are sent from handheld to handheld across the wireless network. The peer-to-peer messages do not pass through a mail server.

focused only on radio infrastructure because current DHS priorities and funding are directed toward management of land mobile radio systems.

Sound guidance is the first step in implementing a secure information system. Incomplete wireless policy, the issuance of weak implementation guidance, and inadequate management oversight may result in sensitive data that cannot be effectively protected. Without adequate controls and implementation procedures for all wireless technologies, malicious users may gain unauthorized access to a network and its data. Establishing and enforcing compliance with a security policy that includes Bluetooth will help mitigate the inherent security risks. Furthermore, wireless networks operating without required security management practices and procedures increase the risk that security controls protecting DHS networks can be circumvented. Finally, components that implement wireless systems without specific requirements and guidelines may not align with DHS wireless goals.

Wireless Networks and Messaging Systems Are Vulnerable

DHS has not established adequate security controls to protect its wireless networks and devices against commonly known security vulnerabilities. To assess the security of wireless within DHS we: (1) used a handheld wireless network scanner to detect rogue⁸ 802.11b devices and evaluate the coverage of the wireless signals broadcast by the access points; (2) used a Bluetooth transceiver to detect the presence of Bluetooth signals; and (3) reviewed security configurations on wireless messaging servers and sampled wireless messaging devices to evaluate the effectiveness of the implemented controls. In assessing the effectiveness of controls implemented on DHS wireless networks and devices, we identified several vulnerabilities regarding 802.11x wireless networks and devices, Bluetooth devices, and wireless messaging systems.

DHS' Wireless Networks Are Susceptible To Monitoring And Eavesdropping

The security controls implemented on DHS' 802.11x wireless networks do not protect against unauthorized access to sensitive data maintained on DHS networks. The DHS components have employed 802.11x technology without effective configuration standards and implementation guidance. Wireless networks operating without a standard wireless configuration or adequate

⁸ A "rogue" access point is one that is accessible to an organization's employees, but is not managed as a part of the approved network. Most rogue access points are installed by employees and not managed by IT administrators.

controls increases the risk that security controls protecting DHS networks can be circumvented.

The 802.11x transmission standard is the most widely installed wireless network technology industry-wide, but many users are unaware of its vulnerabilities. According to industry experts, while some measures are in place to improve security, users or the provider of wireless transmission sites usually neglect these controls.

In October 2003, we requested that DHS components identify their use of wireless technology. As illustrated in Appendix D, four components - Bureau of Citizenship and Immigration Services (CIS), EP&R, TSA, and USCG - said that they were using 802.11x wireless technology. In addition to the four components reporting the use of 802.11x technology, we conducted scans at other selected components: the Bureau of Customs and Border Protection (CBP), DHS Management, and the United States Secret Service (USSS).

We performed random 802.11b detection scans at ten different facilities to identify rogue wireless devices, verify signal coverage for access points, and review configuration settings to evaluate security controls. The four components which reported use of 802.11x technology do not monitor wireless activity and do not have a set schedule to review access point logs to identify unauthorized login attempts or to determine whether rogue devices had been introduced into the network. In addition, during our onsite scans, namely of these four components, we found several 802.11x security vulnerabilities:

- There was no Demilitarized Zone⁹ (DMZ) to separate a wireless network from the wired network at a CIS facility.¹⁰ A wireless network was connected directly to a wired network at the facility. In addition, the local administrator was not aware of the need to establish a DMZ to separate wireless traffic from the wired network.
- For each component using 802.11x technology, there are no intrusion detection systems¹¹ (IDS) installed to monitor wireless activity. IDS can be configured to send a notification to system administrators to

⁹ A “DMZ” is typically a safe area protected by two perimeter firewalls that ensures that users and network traffic do not transverse the two networks without proper authentication and authorization.

¹⁰ Although this is a CIS facility, the site is connected to ICE network infrastructure. In addition to adopting ICE’s security policies at this facility, ICE personnel provide network support to the facility too.

¹¹ An IDS is an effective tool for determining whether unauthorized users are attempting to access, have already accessed, or have compromised the network.

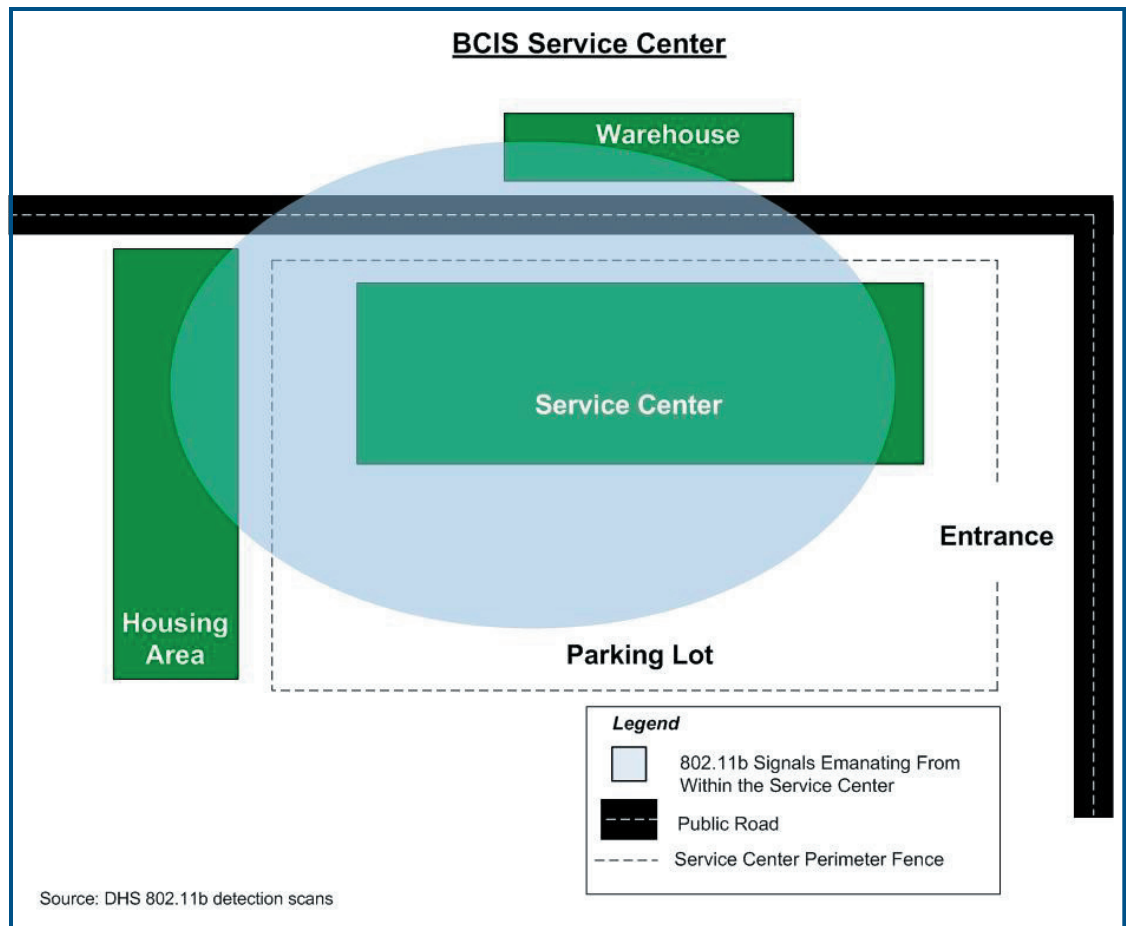
take immediate action and eliminate threats or minimize damage from unauthorized access.

- We identified two rogue wireless access points at a USCG facility. USCG officials told us that they had not performed periodic scans, but they plan to do so once they purchase an 802.11x scanner. Without periodic scans, a malicious or irresponsible user can conceal a rogue device in a closet, under a conference room table, or any hidden area within a building. The rogue device can then be used to intercept traffic between an authorized wireless access point and clients, or allow malicious users unauthorized access to the network. Introducing rogue devices to a network creates significant security vulnerabilities, which bypass security controls and opens a back door to malicious users.
- During our scans, we detected DHS wireless signals broadcasting beyond the physical boundaries, i.e., perimeter walls, at CIS, EP&R, and USCG facilities. Although EP&R and USCG facilities are located within secured compounds, these wireless signals create security vulnerabilities, such as eavesdropping and denial of service¹² attacks. For example, at the CIS Service Center, we detected wireless signals emanating from the facility in the parking lot, on public roads behind the facility, and the surrounding residences.

¹² Denial of service is a form of attacking another computer or company by sending millions or more requests every second causing the network to slow down, cause errors, or shut down.

The following diagram illustrates DHS signals broadcasting beyond the facility's physical boundaries.

Chart 1

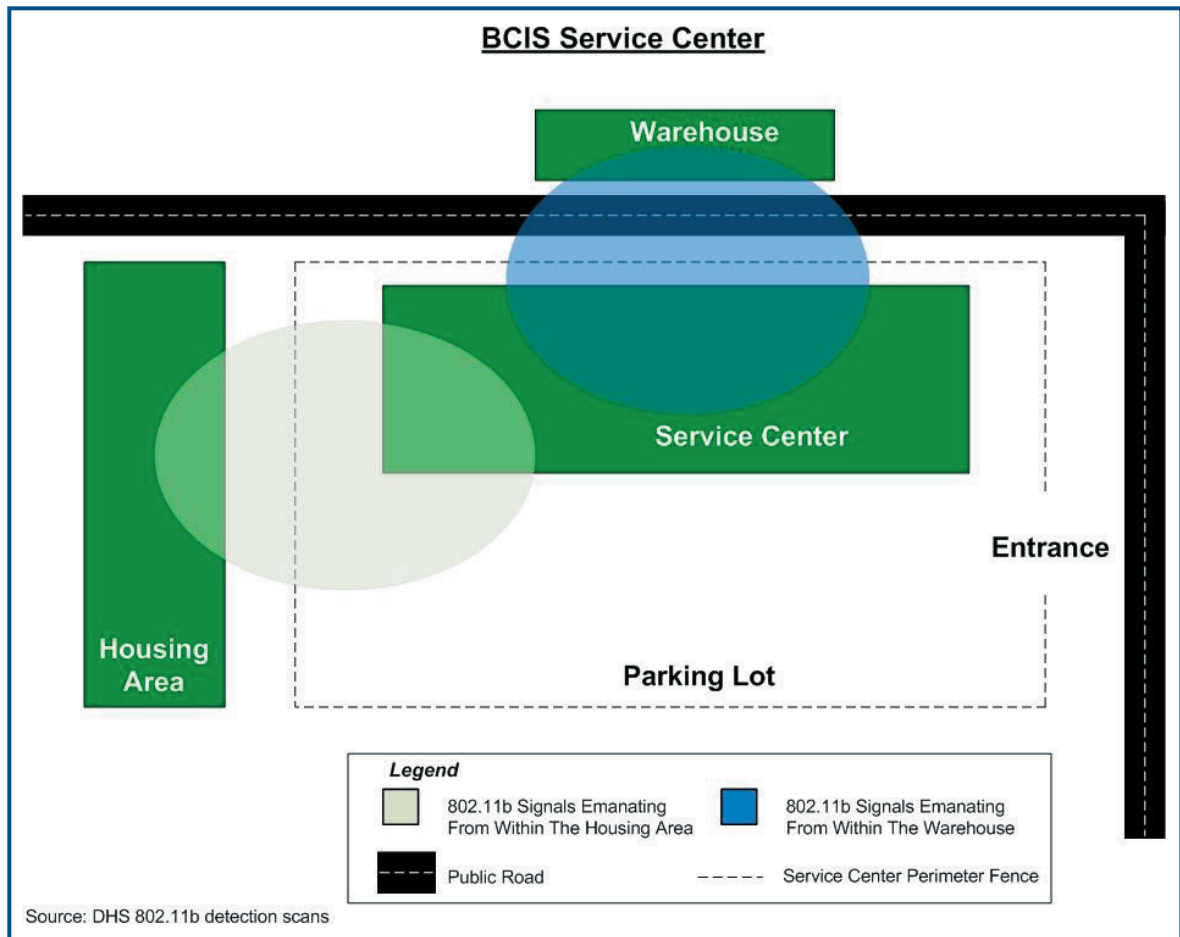


The local CIS administrators said that the DHS signals were detected from outside the facility because wireless access points had been repositioned to the back of the building during a recent expansion. The network administrators did not perform a signal coverage test to determine the proper placement of the access points or to ensure that wireless signals were restricted to the DHS facility.

- We detected non-DHS wireless signals within CIS and CBP facilities. These signals can be used to monitor or gain unauthorized access to DHS wireless networks and sensitive data or to launch denial of service attacks. For example, from within a CIS Service Center facility we detected signals from surrounding residences and businesses.

The following diagram illustrates non-DHS signals broadcasting within the facility's physical boundaries.

Chart 2



The DHS Handbook specifies that maintaining a secure wireless network is an ongoing process that requires greater effort than that required for other networks and systems. In addition, NIST SP 800-48, *Wireless Network Security*, requires that agencies should assess risks more frequently, as well as test and evaluate system security controls when wireless technologies are deployed.

None of the four components using 802.11x technology had applied DHS' minimal security requirements to protect their wireless networks. We discovered that the following controls, required by the DHS Handbook and NIST, were not implemented at one or more sites visited:

-
- Site surveys to place wireless access points strategically to minimize the risks of eavesdropping from unauthorized users.
 - Security tests to evaluate the effectiveness of wireless controls according to the requirements outlined in the NIST SP 800-48.
 - Periodic scans for rogue devices to ensure that unauthorized devices are not introduced to the network.
 - Installation of boundary protection devices, such as firewalls and IDS, to separate wired and wireless networks.
 - Changing the default Wired Equivalent Privacy¹³ (WEP) keys to make them difficult to guess and to minimize unauthorized login attempts.
 - Enabling 128-bit encryption¹⁴ on WEP keys and using robust passwords to increase the level of encryption on the access points and to minimize the threats from unauthorized access.
 - Enabling Media Access Control¹⁵ (MAC) filtering to limit access to legitimate wireless devices.
 - Disabling the broadcast of the Service Set Identifier¹⁶ (SSID) so that this access point identifier is not readily available to the general public.
 - Adopting a “defense in depth”¹⁷ approach, which promotes the application of multiple layers of available security to secure all aspects of a network. In addition, network administrators should receive specialized training on protecting wireless networks.

¹³ “WEP” is a system security protocol (encryption process) specified in the Institute of Electrical and Electronics Engineers 802.11 standards that is designed to provide a wireless local area network with a level of security and privacy comparable to what is usually expected of a wired local area network.

¹⁴ “Encryption” is the conversion of data into a form that cannot be easily understood by unauthorized people. Accordingly, 128-bit encryption is a strong, industry standard method of securing data transmissions.

¹⁵ MAC filtering provides capabilities for restricting access to the wireless local area network based on MAC access control lists that are stored and distributed across many access points. The MAC access control list grants or denies access to a computer using a list of permissions designated by MAC address.

¹⁶ The SSID is a configurable identification that allows clients to communicate to the appropriate base station. With proper configuration, only clients that are configured with the same SSID can communicate with base stations having the same SSID. From a security point of view, the SSID acts as a simple single shared password between base stations and clients.

¹⁷ “Defense in depth” is the concept of protecting a computer network with a series of defensive mechanisms, e.g., if one mechanism fails, another will already be in place to thwart an attack.

Further, of the eight components reviewed, only the USSS had performed 802.11x scans within its facilities. The USSS is currently not using 802.11x technology, but scans for rogue access points as part of its security program requirements.

These weaknesses occurred because, prior to transitioning to DHS, components had already implemented their wireless networks under legacy agencies' security configurations. Wireless controls implemented at the components reviewed were not effective to protect against unauthorized access. Further, there is a lack of awareness among the administrators of the need to implement additional security controls to protect wireless networks.

Because strong controls are not implemented on all of its wireless networks, DHS lacks the ability to prevent unauthorized users from connecting to its networks or to ensure that only legitimate users can access the network resources. Without performing site surveys, DHS cannot ensure that its wireless signals are broadcast only to the intended area and users. Further, when components do not apply NIST's minimal security requirements, DHS does not have assurance that its wireless networks are properly configured and protected against malicious activities. Finally, wireless networks operating without a standardized configuration increase the risk that security controls protecting DHS networks can be circumvented.

Bluetooth Devices Can Be Exploited

Although DHS' policy does not address the use of Bluetooth technology, we identified Bluetooth enabled devices at three of ten components (CIS, USCG, and USSS) scanned. Because end users may not be aware of Bluetooth technology embedded in their devices, equipment can be connected to a network that introduces the security vulnerabilities associated with Bluetooth technology.

Bluetooth technology is built into various technological devices such as headphones, keyboards, digital cameras, printers, projectors, cellular phones, laptop computers, and PDAs - often unknown to the end user. During our scans, we determined that Bluetooth had been enabled on:

- Three laptop computers at a USSS facility. One of these laptop computers was connected to the network, potentially allowing back door access to the network. Neither the user nor security personnel was aware that Bluetooth capability was enabled on the laptop computer. The local administrator

told us that his office performed random scans for 802.11x devices but not for Bluetooth devices.

- Cellular phones at three separate DHS facilities. Although the risk is low, a malicious user can use a Bluetooth enabled cellular phone as a bugging device.

Without policy or procedures to address Bluetooth technology, there is no requirement to test all electronic devices for Bluetooth technology prior to installing any new equipment in a facility or for performing periodic scans for Bluetooth devices.

The NIST SP 800-48 recommends the following controls to protect Bluetooth devices:

- Define the approved uses for Bluetooth devices.
- Prohibit the use of Bluetooth enabled devices in a classified environment.
- Provide users with training as to the vulnerabilities associated with the use of Bluetooth technology.
- Enable device authentication as an extra level of security.
- Enable encryption to encrypt all traffic between devices.
- Enable the device password protection feature.

As Bluetooth continues to gain popularity, DHS must address the security vulnerabilities associated with the use of this technology. Establishing guidelines on servers and devices along with enforcing compliance with security policies can help mitigate the inherent Bluetooth security risks. When Bluetooth vulnerabilities are not addressed, malicious users may gain unauthorized access to a network and its data or launch denial of service attacks.

Wireless Messaging Systems Need More Stringent Controls

DHS has not established adequate security controls to enforce device level management from the server. Consequently, users may disable security configuration settings on their handheld devices. Without stringent controls, DHS

cannot ensure that the sensitive messages processed by its wireless messaging systems are protected from unauthorized accesses and potential misuse.

We identified five components using wireless messaging systems. The CBP, Bureau of Immigration and Customs Enforcement (ICE), DHS Management, and EP&R utilized the Blackberry® Enterprise Server software, while the USCG employed GoodLink™ Server software. To assess the controls over DHS' wireless messaging systems, we randomly sampled wireless devices and reviewed the security configuration settings on the applicable servers.

Only EP&R was using an updated version of Blackberry® software, allowing security controls to be centrally managed from the server. When applied, the server's security settings propagate down and become mandatory for all handheld devices.

DHS Management was using a current version of Blackberry® software, but had not implemented required device controls at the server. The CBP and ICE employed an older version of Blackberry® software, which did not permit device level management from the server. The CBP and ICE Blackberry® servers were configured with weak security settings and did not enforce recommended security controls. Thus, the users could adjust security settings on the device. Specifically, we determined that:

- Password protection was not enabled for individual devices.
- Criteria for password aging and composition were not set at the server, allowing users to create “weak” passwords on the devices.
- Weak encryption was enabled on handheld devices, instead of the recommended strong encryption. Use of weak encryption allows an attacker to easily bypass password protection on a device to gain access to its sensitive contents.
- The Peer-to-Peer feature was not disabled. Wireless messages sent and received between devices are unencrypted, thereby circumventing the Blackberry® software encryption.
- The Internet browsing feature was enabled on handheld devices. Handheld devices that have Internet browsing capability can be susceptible to virus infection and malicious attacks.

-
- The feature to automatically erase the data from the handheld device after a number of unsuccessful logon attempts was not enabled.

The USCG is the only component that uses a GoodLink™ wireless messaging system. The current version of software on the Goodlink™ software permits only limited device level management. Password and device timeout features that protect the device from unauthorized use were enabled through the GoodLink™ desktop software installed on the users' computers; however, users may modify the controls of the desktop software.

The USCG had enabled 128-bit encryption on the GoodLink™ server and on all handheld devices. Further, Peer-to-Peer and Internet browsing features are not available options for GoodLink™ devices. Therefore, this limited functionality does not pose serious vulnerabilities.

Best practices, as presented by the Defense Information Systems Agency¹⁸ and SANS¹⁹, recommend the following controls to secure wireless messaging systems and devices:

- Enable password protection and time-out features.
- Use strong passwords and encryption.
- Disable the Peer-to-Peer feature between devices.
- Disable Internet browsing.
- Enable the feature to automatically erase all data from the handheld device after a number of unsuccessful logon attempts in the event the device is loss or stolen.

Without more stringent controls, DHS cannot ensure that the sensitive messages processed by its wireless messaging systems are protected effectively from unauthorized accesses and potential misuse.

¹⁸ Wireless Security Technical Implementation Guide, Version 1, Release 4, dated January 9, 2003.

¹⁹ SANS is a leader in information security research, certification, and education. The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization.

Wireless Networks Have Not Been Certified and Accredited

DHS' wireless networks and messaging systems are currently operating without C&A. When wireless networks and messaging systems operate without a full C&A, DHS has little assurance that these networks and systems meet a specified set of security requirements.

The primary purpose of C&A is to ensure that adequate security is provided for information collected, processed, transmitted, stored, or disseminated by the systems. Specifically, we determined that:

- CIS, EP&R, USCG, and TSA were using 802.11x wireless networks without a C&A to operate.
- CBP and DHS Management were using wireless messaging systems without a C&A to operate.
- ICE, EP&R, and USCG were using wireless messaging systems under an Interim Authority to Operate.

Without a C&A and Interim Authority to Operate, it is unknown whether systems have met the stringent security requirements established by applicable federal and DHS guidance.

The security certification package presents the results of the security certification and provides the authorizing official with the essential information needed to make a credible risk based decision on whether to authorize operation of the information system. The security certification package contains the following documents: (i) the updated security plan; (ii) the security test and evaluation report; and (iii) the plan of action and milestones.

The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. We identified control weaknesses that may not have occurred had an updated security plan been in place:

- EP&R and DHS Management could not account for all of their wireless messaging devices. Officials said that the devices were lost or stolen.

-
- None of the components included wireless vulnerabilities as part of their security awareness training. Consequently, wireless administrators and users have limited knowledge on the use and protection of wireless devices.
 - DHS management officials maintained two separate wireless messaging inventory lists. One list contained 170 devices while the other identified 534 devices. The security manager was unable to explain this discrepancy.

As previously reported in the *Federal Emergency Management Agency, Government Information Security Reform Act Annual Report For Fiscal Year 2002*, EP&R still does not have a complete listing of all devices with wireless connectivity capabilities. This is a concern because there are many documented information security weaknesses related to wireless connectivity. The deficiencies in security controls, noted above, demonstrate problems with physical security and shortcomings in the security program.

Office of Management and Budget (OMB) Circular A-130 and DHS MD 4300A require formal certification and official management authorization to operate all systems. In addition, all systems shall be re-certified every three years or when a significant change that affects the system's security posture is implemented.

FISMA requires federal agencies to provide mandatory periodic training in computer security awareness and accepted computer security practices for all employees who are involved with the management, use, or operation of a federal computer system within or under the supervision of the federal agency. OMB Circular A-130, Appendix III, issued in 1996, enforces such mandatory training by requiring its completion prior to granting access to the system and through periodic refresher training for continued access.

Having wireless networks and messaging systems operating without a full C&A, DHS has no assurance that these networks and systems meet a specified set of security requirements. The use of wireless technology introduces new security risks to wired networks and the risk for security controls to be circumvented is high on a network or system that is operating without the required C&A. Operating a wireless network and messaging system without C&A could be equivalent of offering intruders easy access to a system's sensitive data.

Recommendations

To enhance the DHS guidance for wireless implementation, we recommend that the CIO:

1. Define the conditions and limitations for using wireless technologies, including Bluetooth, in the DHS security policy.
2. Update the DHS IT Security Program Handbook to include implementation procedures required by NIST SP 800-48 for the use of wireless technologies. In addition, the Chief Information Security Officer should identify what DHS' minimally acceptable system configuration requirements will be and document these requirements in the handbook.
3. Require the National Wireless Management Office to provide the necessary oversight and guidance to align components' wireless programs with DHS' wireless goals.

To protect its wireless networks and messaging systems effectively, we recommend that the CIO:

4. Implement a standardized configuration addressing wireless technologies on DHS networks, consistent with federal security requirements. In addition, the Chief Information Security Officer should require site surveys and wireless scans to verify that DHS' wireless signals are broadcast only to authorized users and areas.

To address the formal information systems review process and authorization to operate, we recommend that the CIO:

5. Complete a C&A for each DHS system according to federal and DHS directives. The Chief Information Security Officer should make certain that the security certification packages contain the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system.

Management Comments and OIG Evaluation

We obtained written comments (Appendix B) on a draft of this report from DHS. DHS agreed with each of our recommendations. Below is a summary of DHS' response to each recommendation and our assessment of the response.

Recommendation 1: Define the conditions and limitations for using wireless technologies, including Bluetooth, in the DHS security policy.

DHS agreed to define the conditions and limitations for using wireless technologies in the DHS security policy. The DHS WMO is currently working with the Chief Information Security Officer to revise MD 4300 along with the associated policy statements, handbooks, and attachments. DHS plans to complete this action by September 30, 2004.

We accept DHS' response to revise the MD 4300 to include existing and emerging wireless technology requirements.

Recommendation 2: Update the DHS IT Security Program Handbook to include implementation procedures required by NIST SP 800-48 for the use of wireless technologies. In addition, the Chief Information Security Officer should identify what DHS' minimally acceptable system configuration requirements will be and document these requirements in the handbook.

DHS agreed and recognized the importance of wireless risk mitigation strategies, as described in NIST Special Publication 800-48. In addition, the DHS WMO formed two functional working groups to address issues related to wireless commercial services. In collaboration with the DHS Chief Information Security Officer, these two working groups bring together the stakeholders that will identify, evaluate, and prepare recommendations regarding new wireless technologies and associated configurations. The resulting guidelines will be implemented and enforced through clearly delegated authority structures presently established within each organization. DHS plans to complete this action by September 30, 2004.

We agree that the formal steps DHS has taken, and plans to take, satisfies the intent of the recommendation.

Recommendation 3: Require the National Wireless Management Office to provide the necessary oversight and guidance to align components' wireless programs with DHS' wireless goals.

DHS agreed with the intent of this recommendation. DHS maintains that the WMO is exercising the appropriate oversight, and is communicating the policies and guidance to the components through its Wireless Working Group. The DHS WMO has formed two working groups that will provide comprehensive oversight and guidance in the area of wireless risk management. Key stakeholders within each organizational component will provide representation and subject matter expertise across three functional areas – (1) policy, planning, and risk management; (2) wireless security in major IT programs; and (3) risk assessment of emerging technologies. These functional areas will report to the parent Wireless Working Group that, in turn, provides recommendations to the DHS WMO. These recommendations will be incorporated, as appropriate, into policy statements and guidelines in MD 4300 and associated handbooks. DHS plans to complete this action by September 30, 2004.

We accept DHS' proposed actions to provide necessary oversight and guidance to align components' wireless programs with DHS' wireless goals. However, during the time of our review and as stated in our report, the WMO was focused solely on land mobile radio systems and was not providing oversight of wireless implementation within DHS. The OIG maintains that DHS, through its WMO, must oversee and manage all DHS wireless functionality.

Recommendation 4: Implement a standardized configuration addressing wireless technologies on DHS networks, consistent with federal security requirements. In addition, the Chief Information Security Officer should require site surveys and wireless scans to verify that DHS' wireless signals are broadcast only to authorized users and areas.

DHS agreed to evaluate its configuration guidelines to ensure compliance with applicable federal security requirements. Wireless site surveys and scans will be conducted on a periodic basis as required by the DHS IT security policy MD 4300. DHS security authorities such as Information System Security Managers, ISSOs, and Network Administrators will develop and enforce DHS policy through routine wireless security vulnerability assessments. DHS plans to complete this action by September 30, 2004.

We accept DHS' response to establish and evaluate new configuration guidelines to ensure compliance with applicable federal standards and to perform wireless site surveys and scans periodically. Once complete, these actions will address the recommendation.

Recommendation 5: Complete a C&A for each DHS system according to federal and DHS directives. The Chief Information Security Officer should make certain that the security certification packages contain the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system.

DHS agreed to implement and maintain a rigorous C&A process for all wireless systems, personal electronic devices, and tactical wireless communication systems. Specifically, the Wireless Security Working Group will coordinate with the DHS WMO and the DHS Chief Information Security Officer to ensure consistency in the development and application of risk management approaches and C&A processes for wireless services and technologies. This collaboration ensures that the DHS WMO is effectively managing the Department's wireless security risks. Additionally, the Designated Accrediting Authority within each organizational component will be responsible for approving the implementation and use of wireless systems at a specified risk level during the C&A process. DHS plans to complete this action by September 30, 2006, contingent upon the availability of funding.

Once complete, these actions will address the recommendation. However, we suggest that DHS strive to complete all system certifications and accreditations sooner than the proposed target date.

Purpose, Scope, and Methodology

The overall objective of this audit was to determine whether DHS developed adequate security policies, established oversight procedures, and implemented sufficient security measures to ensure the networking of wireless devices are secure. Specifically, we determined whether: (1) DHS developed an adequate security policy guide and procedures for wireless networking and devices; (2) security controls have been effectively implemented and configured on DHS' wireless devices and networks to protect against commonly known security vulnerabilities; and, (3) adequate physical controls are implemented to protect portable wireless devices, including sensitive data stored on wireless handheld devices and laptops.

The wireless technologies selected for audit were the 802.11x, IrDA, and Bluetooth. The associated devices using these technologies are the Blackberry®, wireless handheld devices (such as PDAs with wireless capability, wireless mice, and keyboards), and access points (such as routers/hubs). We reviewed these devices because of their increasing popularity, mobility, and the well-known vulnerabilities associated with them.

To accomplish our audit, we conducted fieldwork at the following locations:

- Border and Transportation Security (BTS)²⁰
 - Bureau of Immigration and Customs Enforcement (ICE)
 - Bureau of Customs and Border Protection (CBP)
 - Transportation Security Administration (TSA)
- Bureau of Citizenship and Immigration Services (CIS)
- DHS Management
- Emergency Preparedness and Response (EP&R)
- United States Coast Guard (USCG)
- United States Secret Service (USSS)

During the audit, we used two handheld wireless network scanners to look for authorized, unauthorized, and rogue access points; and access point signal strength on DHS networks:

²⁰ Three DHS components were selected from the BTS directorate.

- The Fluke Networks “WaveRunner™” is a wireless network analyzer that scans for the presence of 802.11b wireless signals.²¹ We conducted non-invasive scans on DHS networks to test compliance with NIST Wireless Network Standards and industry best practices. The WaveRunner™ also verified WEP implementation, correct access point configuration, and Client to access point connections.
- The Berkeley Varitronics Systems Mantis™ Bluetooth Transceiver is a real-time wireless device designed for locating and verifying Bluetooth wireless devices and connections. The scan is non-invasive, non-attacking, and provides information to a tester to determine device identification and capability, signal strength, and approximate location.

We did not examine wireless devices and networks used in classified environments or wireless connectivity through cellular modems and mobile radios during this review. We conducted our audit between October 2003 and January 2004 according to generally accepted government auditing standards. Major contributors to this report are listed in Appendix F.

²¹ The WaveRunner™ does not have the functionality to scan for 802.11a or g protocols. Currently, 802.11a or g protocols do not share the same market usage as 802.11b. According to “In-Stat MDR”, a high-tech market research firm, 802.11b is the predominant wireless protocol.


U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

May 6, 2004

MEMORANDUM FOR: EDWARD G. COLEMAN
DIRECTOR, INFORMATION AND TECHNOLOGY AUDITS
OFFICE OF INSPECTOR GENERAL

FROM: Steven I. Cooper 
Chief Information Officer

SUBJECT: Response to OIG "Draft Audit Report – Inadequate Security Controls
Increase Risk to DHS Wireless Networks (OIG-IT-03-004)" dated
April 2004

Thank you for providing us with a draft copy of the report by the Office of Inspector General (OIG) entitled, "Draft Audit Report – Inadequate Security Controls Increase Risk to DHS Wireless Networks (OIG-IT-03-004)" dated April 2004. We appreciate the opportunity to review, comment, and discuss the issues, findings, and recommendations contained therein.

The Office of the Chief Information Officer (OCIO) appreciates the proactive efforts of the OIG in addressing wireless network security and the constructive recommendations provided in your draft report. The DHS Wireless Management Office (WMO) and Office of the Chief Information Security Officer (CISO), both within the OCIO, are collaborating extensively to address and continuously improve our wireless security posture department-wide. Your report reinforces the importance of their initiatives.

The attachment to this memorandum provides our detailed responses to the findings and recommendations in the subject report.

If you have any questions, please contact Mr. Sean Thrash on 202-772-9948.

Attachment

**Response to the
"Draft Audit Report – Inadequate Security Controls Increase Risk to DHS Wireless
Networks (OIG-IT-03-004)" dated April 2004**

The Department of Homeland Security (DHS) Office of Inspector General (OIG) performed an assessment of the wireless security controls within selected areas of DHS and its organizational components. This audit focused on six components and three subordinate components in evaluating risk management strategies for three specific wireless technologies – (1) 802.11x, (2) IrDA, and (3) Bluetooth. Surveys were conducted on 802.11x and Bluetooth using signal location, identification, and analysis tools.

Based upon its analysis, the OIG identified three primary findings and two secondary findings, and provided five recommendations. This report, findings, and recommendations were reviewed by the DHS Wireless Management Office (WMO) within the Office of the Chief Information Officer (CIO).

Below is a synopsis of the OIG's findings and recommendations, followed by the DHS WMO's response. The DHS WMO responses are shown in italicized font.

Primary Findings

1. DHS wireless policy is incomplete.

Response: The DHS WMO concurs with this finding. The challenges of creating a new department from over 20 separate agencies are reflected in the DHS wireless policy. However, we recognize that we have made progress while concurrently acknowledging that we have not attained all of our goals for wireless security.

2. Implementation procedures can be improved.

Response: The DHS WMO concurs with this finding. The sheer magnitude of the challenges of creating a new department from over 20 separate agencies is reflected in our implementation procedures. However, we continue to refine and improve these procedures, with our goals still set to achieve an appropriate wireless security posture.

3. The National Wireless Management Office is not exercising its full responsibilities.

Response: The DHS WMO disagrees with this finding. The DHS WMO is exercising its responsibilities, oversight, and management. The challenges of creating a new department during the past year are being addressed, and we are making significant progress. We are improving our outreach throughout DHS and

will continue to do so, so that all DHS organizational elements are aware of the existence and responsibilities of the DHS WMO.

In addition, the DHS WMO is working closely with the Chief Information Security Officer to ensure that wireless security policy is properly formulated and promulgated, and is sufficient to ensure DHS' wireless communications. It is the responsibility of the DHS WMO in this partnership to reinforce the requirement to adhere to the published security policies and procedures, and to further heighten awareness regarding wireless security.

Secondary Findings

1. DHS has not established adequate security measures to protect its wireless networks and devices against security risks.

Response: The DHS WMO concurs with this finding.

2. Although DHS security policy requires certification and accreditation (C&A) for its systems to operate, none of the wireless systems reviewed had been certified or accredited.

Response: The DHS WMO concurs with this finding as it pertains to 802.11x, IrDA, and Bluetooth. However, all new tactical wireless systems that are being implemented under the auspices of the DHS WMO are undergoing a thorough C&A.

Recommendations

1. Define the conditions and limitations for using wireless technologies, including Bluetooth, in the DHS security policy.

Response: The DHS WMO concurs with this recommendation. In addition, the conditions and limitations for using satellite communications should also be addressed.

With regards to specific actions underway, the DHS WMO is currently working with the Chief Information Security Officer to revise Management Directive 4300 (MD4300) along with the associated policy statements, handbooks, and attachments. The revision will provide enhancements that proscribe policies and guidelines for procuring, implementing, and using wireless systems, portable electronic devices, and tactical wireless systems in a secure and risk-managed environment. These policies and guidelines will provide the parameters within which wireless technologies may be used. In addition, the policies and guidelines will articulate how components may incorporate emerging wireless standards and technologies. The target date for completion is September 30, 2004.

2. Update the DHS IT Security Program Handbook to include implementation procedures required by NIST SP 800-48 for the use of wireless technologies. In addition, the Chief Information Security Officer should identify what DHS' minimally acceptable system configuration requirements will be and document these requirements in the handbook.

Response: The DHS WMO concurs with this recommendation. In addition, the conditions and limitations for using satellite communications should also be addressed.

The DHS WMO recognizes the importance of wireless risk mitigation strategies, as described in NIST Special Publication 800-48. The 56-point security checklist and the 57-point risk assessment evaluation list provided in the NIST document are referenced in the MD4300 handbooks as the baselines that the organizational components will use to develop wireless system security architectures.

Additionally, the MD4300 handbooks reference and incorporate NIST 800-48 with regards to organizational guidelines for the implementation and use of personal electronic devices. The DHS WMO also recognizes that other industry standards and best practices are important, such as those issued by the Institute of Electrical and Electronics Engineers (IEEE), Project 25 (P25), the American National Standards Institute (ANSI), the National Security Agency (NSA), and by the technology vendor community.

The DHS WMO formed two functional working groups to address issues related to wireless commercial services - Wireless Commercial Services Working Group - and wireless security - Wireless Security Working Group. In collaboration with the DHS Chief Information Security Officer, these two working groups bring together the stakeholders that will identify, evaluate, and prepare recommendations regarding new wireless technologies and associated configurations. The resulting guidelines will be implemented and enforced through clearly delegated authority structures presently established within each organization. The target date for completion is September 30, 2004.

3. Require the National Wireless Management Office to provide the necessary oversight and guidance to align components' wireless programs with DHS' wireless goals.

Response: The DHS WMO concurs with the spirit of this recommendation, although not with the wording. The DHS WMO is exercising the appropriate oversight, and is communicating the policies and guidance to the components through its Wireless Working Group. What is required is a more global, more coordinated effort that transcends the authorities of the DHS WMO. Towards this end, the DHS WMO is working with the Joint Requirements Council (JRC) and

the IT Leadership Council to inform and coordinate the components' wireless efforts.

There remains within the DHS components an organizational resistance to change and a concern that oversight and coordination by the DHS WMO of wireless activities will result in micromanagement and loss of control by the components. This resistance has been an impediment to promulgating oversight and guidance, but it is beginning to diminish.

As noted above, the DHS WMO has formed two working groups that will provide comprehensive oversight and guidance in the area of wireless risk management. Key stakeholders within each organizational component will provide representation and subject matter expertise across three functional areas – (1) policy, planning, and risk management; (2) wireless security in major IT programs; and (3) risk assessment of emerging technologies. These functional areas will report to the parent Wireless Working Group that, in turn, provides recommendations to the DHS WMO. These recommendations will be incorporated, as appropriate, into policy statements and guidelines in MD4300 and associated handbooks. The target date for completion is September 30, 2004.

4. Implement a standardized configuration addressing wireless technologies on DHS networks, consistent with federal security requirements. In addition, the Chief Information Security Officer should require site surveys and wireless scans to verify that DHS' wireless signals are broadcast only to authorized users and areas.

Response: The DHS WMO concurs with this recommendation. In addition, the conditions and limitations for using satellite communications should also be addressed.

As discussed previously, configuration guidelines will be evaluated and recommendations provided by the wireless working groups in conjunction with the DHS Chief Information Security Officer. This coordination will ensure that federal security requirements are considered and applied effectively.

Wireless site surveys and scans will be conducted on a periodic basis as required by the DHS IT security policy MD4300. DHS security authorities such as Information System Security Managers (ISSMs), Information System Security Officers (ISSOs), and Network Administrators will develop and enforce DHS policy through routine wireless security vulnerability assessments. The target date for completion is September 30, 2004.

5. Complete a C&A for each DHS system according to federal and DHS directives. The Chief Information Security Officer should make certain that the security certification packages contain the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system.

Response: The DHS WMO concurs with this recommendation.

DHS will implement and maintain a rigorous C&A process for all wireless systems, personal electronic devices, and tactical wireless communication systems. Specifically, the Wireless Security Working Group will coordinate with the DHS WMO and the DHS Chief Information Security Officer to ensure consistency in the development and application of risk management approaches and C&A processes for wireless services and technologies. This collaboration ensures the DHS WMO is effectively managing the Department's wireless security risks. Additionally, the Designated Accrediting Authority within each organizational component will be responsible for approving the implementation and use of wireless systems at a specified risk level during the C&A process. The target date for completion is September 30, 2006, contingent upon the availability of funding..

Appendix C
Wireless Technology Standards and Functionality

| Wireless Standard | Purpose | Frequency | Range | Speed | Device | Compatibility |
|-------------------------|---|---------------|--|---------------|---|--|
| 802.11a | Wireless network access | 5GHz | 25 to 75 feet indoor; range can be affected by building materials | Up to 54Mbps | Laptop computers, PDAs, cell phones | Not compatible with 802.11b, 802.11g |
| 802.11b | Wireless network access | 2.4GHz | Up to 150 feet indoors; range can be affected by building materials | Up to 11 Mbps | Laptop computers, PDAs, cell phones | Other 2.4GHz devices, like cordless phones, may disrupt connection |
| 802.11g | Wireless network access | 2.4GHz | Up to 150 feet indoors; range can be affected by building materials | Up to 54Mbps | Laptop computers | Other 2.4GHz devices, like cordless phones, may disrupt connection |
| 802.11i | Wireless network access security. Supplementary to MAC layer. Provides alternative to WEP with new encryption methods and authentication procedures | 2.4 – 5.0 GHz | Up to 150 feet indoors; range can be affected by building materials | Up to 54Mbps | Laptop computers, PDAs, cell phones | 802.11a, 802.11b and 802.11g devices |
| Bluetooth 802.15 | Wirelessly connect computer peripherals, such as printers, PDAs, cameras | 2.4GHz | Up to 33 feet (10 meters); range can be affected by building materials | 720Kbps | Printers, cameras, cell phones, headphones, PDAs, other peripherals | Other 2.4GHz devices, like cordless phones, may disrupt connection |

| Components | Wireless Technology | | | | | Draft Security Policy |
|--|---------------------|---------|---------|-----------|--------------------|-----------------------|
| | 802.11a | 802.11b | 802.11g | Bluetooth | Wireless Messaging | |
| DHS Management | | | | X | ◆ | ◆ |
| Bureau of Customs and Border Protection (CBP) | | | | | ◆ | |
| Bureau of Immigration & Customs Enforcement (ICE) | | | | | ◆ | |
| Citizenship & Immigration Services (CIS) | | ◆ | | X | | |
| Emergency Preparedness & Response (EP&R)/FEMA | ◆ | ◆ | ◆ | | ◆ | ◆ |
| Transportation Security Administration (TSA) | ◆ | | | | | ◆ |
| United States Coast Guard (USCG) | | ◆ | | | ◆ | ◆ |
| United States Secret Service (USSS) | | | | X | | |
| ◆ – Disclosed in initial data call. X – Identified during onsite testing. | | | | | | |

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
DHS OIG Liaison
DHS Public Affairs

Office of Management and Budget

Homeland Bureau Chief
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Information Security Audits Division

Edward G. Coleman, Director
Patrick Nadon, IT Audit Manager
Chiu-Tong Tsang, Audit Team Leader
Werner Roberts, Auditor
Lane Melton, Technical Specialist
Ernest Bender, Referencer

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to Department of Homeland Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.